THE STATE of ALASKA

GOVERNOR BILL WALKER

State of Alaska – Department of Health and Social Services

RSA Archer

Authorization Package Framework

Archer Authorization Package Framework

Purpose of Document

This document is an overview of the Department of Health and Social Service's (DHSS) assessment criteria. This criteria is based on the NIST 800-53 Revision 4 information security and compliance framework focusing on NIST 800-66 Revision 1 controls. These controls address systems of a "moderate" risk level's compliance legal requirements such as HIPAA/HITECH. When completed and kept up to date, the requested information noted within this document helps to satisfy many compliance requirements and business needs. For instance, it documents who is responsible for which responsibilities associated with the system, what risk DHSS is assuming through use and support of the system, how DHSS is mitigating that risk, and how DHSS is ensuring that the documented system will have the confidentiality, integrity, and availability needed to fulfill required tasks.

This document provides a list of some of the data required to complete a DHSS RSA Archer authorization package. These packages are a DHSS internally structured web application form of what is commonly referred to as a System Security Plan (SSP). DHSS uses the RSA Archer GRC Assessment and Authorization web application to allow for automated reported and tracking functionality of authorization packages at both a department-wide and individual perspective. The web application is configured, customized, and maintained by DHSS staff per the department's goals. This document is provided as an example of the type of data requested by the web application within an authorization package, but it is not an exact representation of all data as the web application is currently configured to require.

THE STATE of ALASKA

Content

Purpose of Document....1

Content....2

1. Information System Name/Title....6

2. General System Description/Purpose....6

3. Contact Information....6

4. Information System Type....6

5. Information System Categorization:....6

6. Information System Details....6

7. Information System Operational Status....6

7. System Environment....7

8. Privacy Threshold Analysis....7

9. System Interconnections/Information Sharing....9

10. Related Laws/Regulations/Policies....9

11. Minimum Security Controls....10

AC-01: ACCESS CONTROL POLICY AND PROCEDURES....11

AC-02: ACCOUNT MANAGEMENT....13

AC-03: ACCESS ENFORCEMENT....15

AC-04: INFORMATION FLOW ENFORCEMENT....16

AC-05: SEPARATION OF DUTIES....18

AC-06: LEAST PRIVILEGE....19

AC-11: SESSION LOCK....20

AC-12: SESSION TERMINATION....21

AC-17: REMOTE ACCESS....22

AC-19: ACCESS CONTROL FOR MOBILE DEVICES....24

AT-01: SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES....26

AT-02: SECURITY AWARENESS TRAINING....27

AT-03: ROLE-BASED SECURITY TRAINING 28
AT-04: SECURITY TRAINING RECORDS 30
AU-01: AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES 31
AU-02: AUDIT EVENTS 32
AU-03: CONTENT OF AUDIT RECORDS 34
AU-04: AUDIT STORAGE CAPACITY 35
AU-06: AUDIT REVIEW, ANALYSIS, AND REPORTING 36
AU-07: AUDIT REDUCTION AND REPORT GENERATION 37
AU-11: AUDIT RECORD RETENTION 38
CA-01: SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES 39
CA-03: SYSTEM INTERCONNECTIONS 40
CA-07: CONTINUOUS MONITORING 42
CP-01: CONTINGENCY PLANNING POLICY AND PROCEDURES 44
CP-02: CONTINGENCY PLAN 45
CP-03: CONTINGENCY TRAINING 47
CP-04: CONTINGENCY PLAN TESTING 49
CP-06: ALTERNATE STORAGE SITE 51
CP-07: ALTERNATE PROCESSING SITE 52
CP-08: TELECOMMUNICATIONS SERVICES 54
CP-09: INFORMATION SYSTEM BACKUP 55
CP-10: INFORMATION SYSTEM RECOVERY AND RECONSTITUTION 57
IA-02: IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) 58
IA-03: DEVICE IDENTIFICATION AND AUTHENTICATION 60
IA-04: IDENTIFIER MANAGEMENT 61
IA-05: AUTHENTICATOR MANAGEMENT 63
IA-06: AUTHENTICATOR FEEDBACK 65
IR-01: INCIDENT RESPONSE POLICY AND PROCEDURES 66
IR-02: INCIDENT RESPONSE TRAINING 67
IR-03: INCIDENT RESPONSE TESTING 69

IR-04: INCIDENT HANDLING 71
IR-05: INCIDENT MONITORING 72
IR-06: INCIDENT REPORTING 73
IR-07: INCIDENT RESPONSE ASSISTANCE 75
MA-01: SYSTEM MAINTENANCE POLICY AND PROCEDURES 76
MA-02: CONTROLLED MAINTENANCE 77
MA-05: MAINTENANCE PERSONNEL 79
MP-01: MEDIA PROTECTION POLICY AND PROCEDURES 81
MP-02: MEDIA ACCESS 82
MP-04: MEDIA STORAGE 83
MP-05: MEDIA TRANSPORT 85
MP-06: MEDIA SANITIZATION 87
PE-01: PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES 89
PE-02: PHYSICAL ACCESS AUTHORIZATIONS 90
PE-03: PHYSICAL ACCESS CONTROL 92
PE-04: ACCESS CONTROL FOR TRANSMISSION MEDIUM 94
PE-05: ACCESS CONTROL FOR OUTPUT DEVICES 95
PE-06: MONITORING PHYSICAL ACCESS 97
PE-08: VISITOR ACCESS RECORDS 99
PE-17: ALTERNATE WORK SITE 100
PE-18: LOCATION OF INFORMATION SYSTEM COMPONENTS 102
PL-01: SECURITY PLANNING POLICY AND PROCEDURES 103
PS-01: PERSONNEL SECURITY POLICY AND PROCEDURES 104
PS-02: POSITION RISK DESIGNATION 105
PS-03: PERSONNEL SCREENING 107
PS-04: PERSONNEL TERMINATION 109
PS-05: PERSONNEL TRANSFER 111
PS-06: ACCESS AGREEMENTS 113
PS-07: THIRD-PARTY PERSONNEL SECURITY 115

PS-08: PERSONNEL SANCTIONS 117
RA-01: RISK ASSESSMENT POLICY AND PROCEDURES 118
RA-02: SECURITY CATEGORIZATION 119
SA-04: ACQUISITION PROCESS 121
SA-09: EXTERNAL INFORMATION SYSTEM SERVICES 123
SC-08: TRANSMISSION CONFIDENTIALITY AND INTEGRITY 125
SC-12: CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT 127
SI-01: SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES 129
SI-03: MALICIOUS CODE PROTECTION 130
SI-04: INFORMATION SYSTEM MONITORING 132
SI-05: SECURITY ALERTS, ADVISORIES, AND DIRECTIVES 134
SI-07: SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY 136
SI-08: SPAM PROTECTION 137
SI-10: INFORMATION INPUT VALIDATION 138
Appendix A – Acronyms and Abbreviations 139

1. Information System Name/Title

<Authorization Package Name>

<Acronym>

2. General System Description/Purpose

<Program Staff Description of the M*ission* or P*urpose* of the System>

3. Contact Information

Name, Title, Email, Phone for:

- Information Owner (IO)
- Program Manager (PM)
- Security Designee (SD)
- Technical Contact(s) (TC)
- Other Contacts

4. Information System Type

<Information System / Program or Site>

5. Information System Categorization:

Security Category: <Low/Moderate/High>

6. Information System Details

- Connectivity: <Networked or Standalone>
- Loss of Life: <Yes or No, Lack of Availability Leading to Death>
- Daily Estimated Cost From an Outage: <Does Not Have to Be Exact, a Range Will Suffice>

7. Information System Operational Status

Operational Status:	<Production / In Development>
Financial System:	<Yes/No>
Critical Infrastructure:	<Yes/No>

Mission Critical: <Yes/No>
FISMA Reportable: <Yes/No>

7. System Environment

- Business Process Diagram
- Boundary Description
- Boundary Diagram
- Network Diagram
- Data Flow Diagram
- Software List
    - Software Name
    - Software Version Number
- Hardware List
    - Device Name
    - Host Name (if applicable)
    - IP Address
- Database List
- Most Recent Vulnerability Scan Report
- Patching and Support Information
- Regular Maintenance Window Schedule

8. Privacy Threshold Analysis

PTA-1: Select an Information System status (select one):

- This is a new development effort
- This is an existing project

PTA-2: Does the Information System collect, maintain, use or disseminate personally identifiable information on any of the following parties (select all that apply):

- This program does not collect any personally identifiable information
- Employees
- Contractors
- Members of the public
- Other

PTA-3: Does the Information System intend to collect, generate, or retain any of the following information considered PII, PHI, CJIS or confidential on individuals (select all that apply):

- None of these values apply
- Name
- Birth Information (Date and/or Place of birth)
- Admission Date
- Discharge Date
- Date of Death
- Medical Record Numbers
- Health Plan
- Beneficiary Numbers
- Financial data (credit card numbers, bank account numbers, etc.)
- Certificate/License Numbers
- Criminal History
- Employment History (Wage Information)
- Biometric Information (fingerprints, voice prints, iris scans, DNA, etc.)
- Full face photographic images and any comparable images
- Personal information (mailing and/or residency address, e-mail, phone numbers, fax numbers, etc.)
- Other unique identifying number, characteristic or code

PTA-4: Does the Information System use or collect Social Security Numbers (SSN)? This includes truncated SSN's (e.g. last 4 digits) (select one):

- No
- Yes

PTA-5: Does the system connect, receive, or share information with any other Information System (select one):

- No
- Yes

PTA-6: Does the Information System connect, receive, or share information with any external systems (select one):

- No
- Yes

PTA-7: Are there regular (i.e. periodic, recurring, etc.) data extractions from the Information System (select one):

- No
- Yes

PTA-8: Who has access to your system that is not a workforce member of DHSS, such as other State Departments, Grantees, Providers, Public, etc. (select all that apply):

- Contractors
- Federal Government
- Grantees

- Other State Governments
- Other State of Alaska Departments
- Public
- Service Providers
- State of Alaska Courts
- State of Alaska Legislature
- Vendors

PTA-9: What procedures are in place to determine which users may access the information and how does the project determine who has access:

<narrative answer required>

PTA-10: How does the project team review information sharing agreements, MOU's, new uses of the information, new access to the system by organizations within the department and outside:

<narrative answer required>

9. System Interconnections/Information Sharing

Interconnection Name	Type	Manual or External / Networked	Connection Protocol(s) Used	Connecting Information System	Inbound or Outbound	Purpose

10. Related Laws/Regulations/Policies

(Double-Click on each box to change "marked" status)

☐	Alaska Statutes	☐	DHSS Policies	☐	HIPAA/HITECH (EPHI)	☐	CJIS Security Policy

☐	Federal Statutes	☐	SoA Policies	☐	IRS PUB 1075 (FTI)	☐	PCI DSS
		☐	Alaska Personal Information Protection Act (PI)	☐	CMS MARS-E	☐	Other

11. Minimum Security Controls

TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

AC-01: ACCESS CONTROL POLICY AND PROCEDURES

Number
AC-01

Family
Access Control

Name
ACCESS CONTROL POLICY AND PROCEDURES

Baseline
Low; Moderate; High

Description
The organization:

a. Develops, documents, and disseminates to applicable personnel:
   1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the access control policy and associated access controls; and
b. Reviews and updates the current:
   1. Access control policy (as necessary) within every three hundred sixty-five (365) days; and
   2. Access control procedures (as necessary) within every three hundred sixty-five (365) days.

NIST Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Related control: PM-9.

References: NIST Special Publications 800-12, 800-100.

AC-02: ACCOUNT MANAGEMENT

Number
AC-02

Family
Access Control

Name
ACCOUNT MANAGEMENT

Baseline
Low; Moderate; High

Description
The organization:

a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: individual, group, system, application, guest/anonymous, emergency, and temporary;
b. Assigns account managers for information system accounts;
c. Establishes conditions for group and role membership;
d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e. Requires approvals by defined personnel or roles for requests to create information system accounts;
f. Creates, enables, modifies, disables, and removes information system accounts in accordance with organizational standards and procedures;
g. Monitors the use of, information system accounts;
h. Notifies account managers:
    1. When accounts are no longer required;
    2. When users are terminated or transferred; and
    3. When individual information system usage or need-to-know changes;
i. Authorizes access to the information system based on:
    1. A valid access authorization;
    2. Intended system usage; and
    3. Other attributes as required by the organization or associated missions/business functions;
j. Reviews accounts for compliance with account management requirements within every one hundred eighty (180) days; and
k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

NIST Guidance

Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training.

Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13.

References: None.

DHSS Guidance

AC-03: ACCESS ENFORCEMENT

Number
AC-03

Family
Access Control

Name
ACCESS ENFORCEMENT

Baseline
Low; Moderate; High

Description
The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

NIST Guidance
Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level and recognizing that information systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security.

Related controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PE-3.

References: None.

DHSS Guidance

AC-04: INFORMATION FLOW ENFORCEMENT

Number
AC-04

Family
Access Control

Name
INFORMATION FLOW ENFORCEMENT

Baseline
Low; Moderate; High

Description
The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on applicable policy.

NIST Guidance
Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example: (i) prohibiting information transfers between interconnected systems (i.e., allowing access only); (ii) employing hardware mechanisms to enforce one-way information flows; and (iii) implementing trustworthy regrading mechanisms to reassign security attributes and security labels.

Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header

information, or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 22 primarily address cross-domain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, for example, high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf information technology products.

Related controls: AC-3, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.

References: Web: ucdmo.gov.

DHSS Guidance

AC-05: SEPARATION OF DUTIES

Number
AC-05

Family
Access Control

Name
SEPARATION OF DUTIES

Baseline
Low; Moderate; High

Description
The organization:

a. Separates duties of individuals as necessary to prevent malevolent activity without collusion;
b. Documents separation of duties of individuals; and
c. Defines information system access authorizations to support separation of duties.

NIST Guidance
Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions.

Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.

References: None.

DHSS Guidance

AC-06: LEAST PRIVILEGE

Number
AC-06

Family
Access Control

Name
LEAST PRIVILEGE

Baseline
Low; Moderate; High

Description
The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

NIST Guidance
Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems.

Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.

References: None.

DHSS Guidance

AC-11: SESSION LOCK

Number
AC-11

Family
Access Control

Name
SESSION LOCK

Baseline
Moderate; High

Description
The information system:

a. Prevents further access to the system by initiating a session lock after fifteen (15) minutes of inactivity or upon receiving a request from a user; and
b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

NIST Guidance
Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays.

Related control: AC-7.

References: OMB Memorandum 06-16.

DHSS Guidance

AC-12: SESSION TERMINATION

Number
AC-12

Family
Access Control

Name
SESSION TERMINATION

Baseline
Moderate; High

Description
The information system automatically terminates a user session after fifteen (15) minutes of inactivity.

NIST Guidance
This control addresses the termination of user-initiated logical sessions in contrast to SC-10 which addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information system use.

Related controls: SC-10, SC-23.

References: None.

DHSS Guidance

AC-17: REMOTE ACCESS

Number
AC-17

Family
Access Control

Name
REMOTE ACCESS

Baseline
Low; Moderate; High

Description
The organization:

a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
b. Authorizes remote access to the information system prior to allowing such connections.

NIST Guidance
Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to information systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the formats for such authorization. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote connections is addressed in AC-3.

Related controls: AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10, SI-4.

References: NIST Special Publications 800-46, 800-77, 800-113, 800-114, 800-121.

DHSS Guidance

AC-19: ACCESS CONTROL FOR MOBILE DEVICES

Number
AC-19

Family
Access Control

Name
ACCESS CONTROL FOR MOBILE DEVICES

Baseline
Low; Moderate; High

Description
The organization:

a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
b. Authorizes the connection of mobile devices to organizational information systems.

NIST Guidance
A mobile device is a computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, E-readers, and tablets. Mobile devices are typically associated with a single individual and the device is usually in close proximity to the individual; however, the degree of proximity can vary depending upon on the form factor and size of the device. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of desktop systems, depending upon the nature and intended purpose of the device. Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different classes/types of such devices. Usage restrictions and specific implementation guidance for mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Organizations are cautioned that the need to provide adequate security for mobile devices goes beyond the requirements in this control. Many safeguards and countermeasures for mobile devices are reflected in other security controls in the catalog allocated in the initial control baselines as starting points for the development of

security plans and overlays using the tailoring process. There may also be some degree of overlap in the requirements articulated by the security controls within the different families of controls. AC-20 addresses mobile devices that are not organization-controlled.

Related controls: AC-3, AC-7, AC-18, AC-20, CA-9, CM-2, IA-2, IA-3, MP-2, MP-4, MP-5, PL-4, SC-7, SC-43, SI-3, SI-4.

References: OMB Memorandum 06-16; NIST Special Publications 800-114, 800-124, 800-164.

DHSS Guidance

AT-01: SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Number
AT-01

Family
Awareness and Training

Name
SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Baseline
Low; Moderate; High

Description
The organization:

a. Develops, documents, and disseminates to applicable personnel:
   1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and
b. Reviews and updates the current:
   1. Security awareness and training policy within every three hundred sixty-five (365) days; and
   2. Security awareness and training procedures within every three hundred sixty-five (365) days.

NIST Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AT family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Related control: PM-9.

References: NIST Special Publications 800-12, 800-16, 800-50, 800-100.

DHSS Guidance

AT-02: SECURITY AWARENESS TRAINING

Number
AT-02

Family
Awareness and Training

Name
SECURITY AWARENESS TRAINING

Baseline
Low; Moderate; High

Description
The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

a. As part of initial training for new users;
b. When required by information system changes; and
c. Within every three hundred sixty-five (365) days thereafter.

NIST Guidance
Organizations determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

Related controls: AT-3, AT-4, PL-4.

References: C.F.R. Part 5 Subpart C (5 C.F.R 930.301); Executive Order 13587; NIST Special Publication 800-50.

DHSS Guidance

AT-03: ROLE-BASED SECURITY TRAINING

Number
AT-03

Family
Awareness and Training

Name
ROLE-BASED SECURITY TRAINING

Baseline
Low; Moderate; High

Description
The organization provides role-based security training to personnel with assigned security roles and responsibilities:

a. Before authorizing access to the information system or performing assigned duties;
b. When required by information system changes; and
c. Within every three hundred sixty-five (365) days thereafter.

NIST Guidance
Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations and the information systems to which personnel have authorized access. In addition, organizations provide enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs. Role-based security training also applies to contractors providing services to federal agencies.

Related controls: AT-2, AT-4, PL-4, PS-7, SA-3, SA-12, SA-16.

References: C.F.R. Part 5 Subpart C (5 C.F.R. 930.301); NIST Special Publications 800-16, 800-50.

AT-04: SECURITY TRAINING RECORDS

Number
AT-04

Family
Awareness and Training

Name
SECURITY TRAINING RECORDS

Baseline
Low; Moderate; High

Description
The organization:

a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and
b. Retains individual training records for a minimum of five (5) years.

NIST Guidance
Documentation for specialized training may be maintained by individual supervisors at the option of the organization.

Related controls: AT-2, AT-3, PM-14.

References: None.

DHSS Guidance

AU-01: AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Number
AU-01

Family
Audit and Accountability

Name
AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Baseline
Low; Moderate; High

Description
The organization:

a. Develops, documents, and disseminates to applicable personnel:
   1. An audit and accountability policy that addresses purpose, people, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and
b. Reviews and updates the current:
   1. Audit and accountability policy within every three hundred sixty-five (365) days; and
   2. Audit and accountability procedures within every three hundred sixty-five (365) days.

NIST Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AU family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Related control: PM-9.

References: NIST Special Publications 800-12, 800-100.

DHSS Guidance

AU-02: AUDIT EVENTS

Number
AU-02

Family
Audit and Accountability

Name
AUDIT EVENTS

Baseline
Low; Moderate; High

Description
The organization:

a. Determines that the information system is capable of auditing the following events:
   1. Server alerts and error messages;
   2. Log onto system;
   3. Log off system;
   4. Change of password;
   5. All system administrator commands, while logged on as system administrator;
   6. Switching accounts or running privileged actions from another account, (e.g., Linux/UNIX SU or Windows RunAs);
   7. Creation or modification of super-user groups;
   8. Subset of security administrator commands, while logged on in the security administrator role;
   9. Subset of system administrator commands, while logged on in the user role;
   10. Clearing of the audit log file;
   11. Startup and shutdown of audit functions;
   12. Use of identification and authentication mechanisms (e.g., user ID and password);
   13. Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su);
   14. Remote access outside of the corporate network communication channels (e.g., modems, dedicated Virtual Private Network) and all dial-in access to the system;
   15. Changes made to an applications or database by a batch file;
   16. Application-critical record changes;
   17. Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility);
   18. User log-on and log-off (successful or unsuccessful);
   19. System shutdown and reboot;
   20. System errors;
   21. Application shutdown;
   22. Application restart;

23. Application errors;
24. Security policy modifications; and
25. Printing sensitive information;

b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
d. Determines that the following events are to be audited within the information system: All applicable events listed under AU-02 a, audited on a continuous basis or in response to specific situations as appropriate based on current threat information and ongoing assessment of risk.

NIST Guidance

An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs. Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage. In determining the set of auditable events, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are audited at a given point in time. For example, organizations may determine that information systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. Auditing requirements, including the need for auditable events, may be referenced in other security controls and control enhancements. Organizations also include auditable events that are required by applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of auditable events, the auditing necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented architectures.

Related controls: AC-6, AC-17, AU-3, AU-12, MA-4, MP-2, MP-4, SI-4.

References: NIST Special Publication 800-92; Web: csrc.nist.gov/pcig/cig.html, idmanagement.gov.

DHSS Guidance

AU-03: CONTENT OF AUDIT RECORDS

Number
AU-03

Family
Audit and Accountability

Name
CONTENT OF AUDIT RECORDS

Baseline
Low; Moderate; High

Description
The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

NIST Guidance
Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred).

Related controls: AU-2, AU-8, AU-12, SI-11.

References: None.

DHSS Guidance

AU-04: AUDIT STORAGE CAPACITY

Number
AU-04

Family
Audit and Accountability

Name
AUDIT STORAGE CAPACITY

Baseline
Low; Moderate; High

Description
The organization allocates audit record storage capacity in accordance with reducing the likelihood that storage capacity will be exceeded.

NIST Guidance
Organizations consider the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability.

Related controls: AU-2, AU-5, AU-6, AU-7, AU-11, SI-4.

References: None.

DHSS Guidance

AU-06: AUDIT REVIEW, ANALYSIS, AND REPORTING

Number
AU-06

Family
Audit and Accountability

Name
AUDIT REVIEW, ANALYSIS, AND REPORTING

Baseline
Low; Moderate; High

Description
The organization:

a. Reviews and analyzes information system audit records regularly for indications of inappropriate or unusual activity; and
b. Reports findings to the Department Chief Security Officer.

NIST Guidance
Audit review, analysis, and reporting covers information security-related auditing performed by organizations including, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of VoIP. Findings can be reported to organizational entities that include, for example, incident response team, help desk, information security group/department. If organizations are prohibited from reviewing and analyzing audit information or unable to conduct such activities (e.g., in certain national security applications or systems), the review/analysis may be carried out by other organizations granted such authority.

Related controls: AC-2, AC-3, AC-6, AC-17, AT-3, AU-7, AU-16, CA-7, CM-5, CM-10, CM-11, IA-3, IA-5, IR-5, IR-6, MA-4, MP-4, PE-3, PE-6, PE-14, PE-16, RA-5, SC-7, SC-18, SC-19, SI-3, SI-4, SI-7.

References: None.

DHSS Guidance

AU-07: AUDIT REDUCTION AND REPORT GENERATION

Number
AU-07

Family
Audit and Accountability

Name
AUDIT REDUCTION AND REPORT GENERATION

Baseline
Moderate; High

Description
The information system provides an audit reduction and report generation capability that:

a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
b. Does not alter the original content or time ordering of audit records.

NIST Guidance
Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit reduction and report generation capabilities do not always emanate from the same information system or from the same organizational entities conducting auditing activities. Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the information system can generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the timestamp in the record is insufficient.

Related control: AU-6.

References: None.

DHSS Guidance

AU-11: AUDIT RECORD RETENTION

Number
AU-11

Family
Audit and Accountability

Name
AUDIT RECORD RETENTION

Baseline
Moderate; High

Description
The organization retains audit records for at least ninety (90) days and archives old records for six (6) years to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

NIST Guidance
Organizations retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention.

Related controls: AU-4, AU-5, AU-9, MP-6.

References: None.

DHSS Guidance

CA-01: SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES

Number
CA-01

Family
Security Assessment and Authorization

Name
SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES

Baseline
Low; Moderate; High

Description
The organization:

a. Develops, documents, and disseminates to applicable personnel:
   1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and
b. Reviews and updates the current:
   1. Security assessment and authorization policy within three hundred sixty-five (365) days; and
   2. Security assessment and authorization procedures within three hundred sixty-five (365) days.

NIST Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Related control: PM-9.

References: NIST Special Publications 800-12, 800-37, 800-53A, 800-100.

DHSS Guidance

CA-03: SYSTEM INTERCONNECTIONS

Number
CA-03

Family
Security Assessment and Authorization

Name
SYSTEM INTERCONNECTIONS

Baseline
Low; Moderate; High

Description
The organization:

a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;
b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
c. Reviews and updates Interconnection Security Agreements within three hundred sixty-five (365) days or when there are changes to the connection.

NIST Guidance
This control applies to dedicated connections between information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing. Organizations carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within organizations and external to organizations. Authorizing officials determine the risk associated with information system connections and the appropriate controls employed. If interconnecting systems have the same authorizing official, organizations do not need to develop Interconnection Security Agreements. Instead, organizations can describe the interface characteristics between those interconnecting systems in their respective security plans. If interconnecting systems have different authorizing officials within the same organization, organizations can either develop Interconnection Security Agreements or describe the interface characteristics between systems in the security plans for the respective systems. Organizations may also incorporate Interconnection Security Agreement information into formal contracts, especially for interconnections established between federal agencies and nonfederal (i.e., private sector) organizations. Risk considerations also include information systems sharing the same networks. For certain technologies (e.g., space, unmanned aerial vehicles, and medical devices), there may be specialized connections in place during preoperational testing. Such connections may require Interconnection Security Agreements and be subject to additional security controls.

Related controls: AC-3, AC-4, AC-20, AU-2, AU-12, AU-16, CA-7, IA-3, SA-9, SC-7, SI-4.

References: FIPS Publication 199; NIST Special Publication 800-47.

DHSS Guidance

What systems if any does your application interact with?

Such as: Splunk, Active Directory, SQL, Oracle, the MCI Cube, etc?

By enumerating the other systems your application interacts with you get insight into the risks you inherit from other people and systems.

CA-07: CONTINUOUS MONITORING

Number
CA-07

Family
Security Assessment and Authorization

Name
CONTINUOUS MONITORING

Baseline
Low; Moderate; High

Description
The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

a. Establishment of organizationally defined metrics to be monitored;
b. Establishment of defined frequencies for monitoring and defined frequencies for assessments supporting such monitoring;
c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
e. Correlation and analysis of security-related information generated by assessments and monitoring;
f. Response actions to address results of the analysis of security-related information; and
g. Reporting the security status of organization and the information system to the Information Owner, IT management, and the Department Chief Security Officer monthly.

NIST Guidance
Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Continuous monitoring programs also allow organizations to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies. Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization

packages, hardware/software/firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of information systems.

Related controls: CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA-11, SA-12, SI-2, SI-4.

References: OMB Memorandum 11-33; NIST Special Publications 800-37, 800-39, 800-53A, 800-115, 800-137; US-CERT Technical Cyber Security Alerts; DoD Information Assurance Vulnerability Alerts.

DHSS Guidance

This is a complex multifaceted control. The core premise is that your system be kept up to date in the ever changing environment that we live in. This includes patching (Operating System, Software, etc), code updates, vulnerability scanning, and keeping abreast of hacker activity. Luckily you're not alone!

Responsibility for meeting this control is shared with the Department Security Office, Network Services (If applicable), Business Applications (If applicable), and any business partners you may have.

Here are directions for each specific control sub-group.

A. The DSO has taken care of this control. DHSS systems must routinely use a static code analysis scanner (Veracode), and a Network vulnerability scanner (McAfee Vulnerability Manager). If your application is hosted and or maintained by a third party you'll need to what tools they use to perform code analysis and network scanning.

B. DHSS policy directs scanning to occur every 30 or 90 days depending on if the system is designated as critical or non-critical. Additionally scanning should occur after ever system revision.

C. as the system undergoes significant updates and revisions security controls will need to be reviewed. Significant updates generally include new major features, major version updates, or system redesigns.

D. DHSS monitors a number of different channels to keep abreast of the changing nature of our threat environment. These include but are not limited to partnerships with Law Enforcement, Security Trade Organizations, and Professional communities. The security designee should maintain contacts within their own professional community to understand what threats are immediately relevant.

E. The department meets this requirement through active partnership between the DSO, Security Designees, and applicable business partners.

F,G. are handled by DHSS policy on continuous monitoring (see policy#)

CP-01: CONTINGENCY PLANNING POLICY AND PROCEDURES

Number
CP-01

Family
Contingency Planning

Name
CONTINGENCY PLANNING POLICY AND PROCEDURES

Baseline
Low; Moderate; High

Description
The organization:

a. Develops, documents, and disseminates to applicable personnel:
   1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and
b. Reviews and updates the current:
   1. Contingency planning policy within every three hundred sixty-five (365) days; and
   2. Contingency planning procedures within every three hundred sixty-five (365) days.

NIST Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Related control: PM-9.

References: Federal Continuity Directive 1; NIST Special Publications 800-12, 800-34, 800-100.

DHSS Guidance

CP-02: CONTINGENCY PLAN

Number
CP-02

Family
Contingency Planning

Name
CONTINGENCY PLAN

Baseline
Low; Moderate; High

Description
The organization:

a. Develops a contingency plan for the information system that:
    1. Identifies essential missions and business functions and associated contingency requirements;
    2. Provides recovery objectives, restoration priorities, and metrics;
    3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
    4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
    5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
    6. Is reviewed and approved by the Information Owner and Department Chief Security Officer;
b. Distributes copies of the contingency plan to the Information Owner, Department Chief Security Officer, contingency plan coordinator, and other stakeholders identified within the contingency plan;
c. Coordinates contingency planning activities with incident handling activities;
d. Reviews the contingency plan for the information system within every three hundred sixty-five (365) days;
e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f. Communicates contingency plan changes to stakeholders; and
g. Protects the contingency plan from unauthorized disclosure and modification.

NIST Guidance
Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and

firmware development can be an effective means of achieving information system resiliency. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired. Information system recovery objectives reflect applicable laws, Executive Orders, directives, policies, standards, regulations, and guidelines. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission and/or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information systems. Actions addressed in contingency plans include, for example, orderly/graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident.

Related controls: AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5, PM-8, PM-11.

References: Federal Continuity Directive 1; NIST Special Publication 800-34.

DHSS Guidance

Contingency planning is a significant activity. What do you do when the system goes down, what do you do when there is a power outage, what impact if any will happen to your clients?

The good news is that if you use the DHSS data center most of the technical details have been taken care of by the networking team, however only you can answer to what your business needs and client's requirements are.

CP-03: CONTINGENCY TRAINING

Number
CP-03

Family
Contingency Planning

Name
CONTINGENCY TRAINING

Baseline
Low; Moderate; High

Description
The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

a. Within ninety (90) days of assuming a contingency role or responsibility;
b. When required by information system changes; and
c. Within every three hundred sixty-five (365) days thereafter.

NIST Guidance
Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to set up information systems at alternate processing and storage sites; and managers/senior leaders may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles/responsibilities reflects the specific continuity requirements in the contingency plan.

Related controls: AT-2, AT-3, CP-2, IR-2.

References: Federal Continuity Directive 1; NIST Special Publications 800-16, 800-50.

DHSS Guidance
Historically DHSS has not done a very good job of meeting this control, so if this is risk assumption for your division you're in good company.

As an aspirational goal this is where you want to be, performing some kind of recovery training once a quarter. If you're performing it once a year, you're probably okay. If no one is trained in what to do during an emergency

then you are going to have a hard time if the power, or the internet, or a serious event like an earth quake occurs.

CP-04: CONTINGENCY PLAN TESTING

Number
CP-04

Family
Contingency Planning

Name
CONTINGENCY PLAN TESTING

Baseline
Low; Moderate; High

Description
The organization:

a. Tests the contingency plan for the information system within every three hundred sixty-five (365) days using functional exercises to determine the effectiveness of the plan and the organizational readiness to execute the plan;
b. Reviews the contingency plan test results; and
c. Initiates corrective actions, if needed.

NIST Guidance
Methods for testing contingency plans to determine the effectiveness of the plans and to identify potential weaknesses in the plans include, for example, walk-through and tabletop exercises, checklists, simulations (parallel, full interrupt), and comprehensive exercises. Organizations conduct testing based on the continuity requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals arising due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions.

Related controls: CP-2, CP-3, IR-3.

References: Federal Continuity Directive 1; FIPS Publication 199; NIST Special Publications 800-34, 800-84.

DHSS Guidance
Historically DHSS has not done a very good job of meeting this control, so if this is risk assumption for your division you're in good company.

Working in Alaska there is a very good chance that you get the opportunity to test out your contingency plans at least yearly through network and power outages. Formalizing the process and performing an after action review of some kind will help to work out the kinks in any plan. A good place to start is just in making sure people know

who to call when things go wrong. These events do not have to be intrusive and can be spot checks, or table top exercises that take less than 30 mins.

CP-06: ALTERNATE STORAGE SITE

Number
CP-06

Family
Contingency Planning

Name
ALTERNATE STORAGE SITE

Baseline
Moderate; High

Description
The organization:

a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and
b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

NIST Guidance
Alternate storage sites are sites that are geographically distinct from primary storage sites. An alternate storage site maintains duplicate copies of information and data in the event that the primary storage site is not available. Items covered by alternate storage site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination of delivery/retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems.

Related controls: CP-2, CP-7, CP-9, CP-10, MP-4.

References: NIST Special Publication 800-34.

DHSS Guidance
If you use the DHSS data centers then this control is managed for you by DHSS networking. If you host servers in your local offices, or utilize a third party then you'll need to contact them to understand if you meet the control requirements above.

CP-07: ALTERNATE PROCESSING SITE

Number
CP-07

Family
Contingency Planning

Name
ALTERNATE PROCESSING SITE

Baseline
Low; Moderate; High

Description
The organization:

a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of information system operations for essential missions/business functions within a resumption time period consistent with the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) defined by the Information Owner and documented in the authorization package and contingency plan, when the primary processing capabilities are unavailable;
b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and
c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

NIST Guidance
Alternate processing sites are sites that are geographically distinct from primary processing sites. An alternate processing site provides processing capability in the event that the primary processing site is not available. Items covered by alternate processing site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination for the transfer/assignment of personnel. Requirements are specifically allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems.

Related controls: CP-2, CP-6, CP-8, CP-9, CP-10, MA-6.

References: NIST Special Publication 800-34.

DHSS Guidance

If you use the DHSS data centers then this control is managed for you by DHSS networking. If you host servers in your local offices, or utilize a third party then you'll need to contact them to understand if you meet the control requirements above.

CP-08: TELECOMMUNICATIONS SERVICES

Number
CP-08

Family
Contingency Planning

Name
TELECOMMUNICATIONS SERVICES

Baseline
Moderate; High

Description
The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within a resumption time period consistent with the Recovery Time Objectives (RTO) defined by the Information Owner and documented in the authorization package and contingency plan, when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

NIST Guidance
This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential missions/business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary/alternate sites. Alternate telecommunications services include, for example, additional organizational or commercial ground-based circuits/lines or satellites in lieu of ground-based communications. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements.

Related controls: CP-2, CP-6, CP-7.

References: NIST Special Publication 800-34; National Communications Systems Directive 3-10; Web: tsp.ncs.gov.

DHSS Guidance
What do you do when the phones, email, or the internet goes down? Do you have phone trees? How long can you go without desk phones or email?

CP-09: INFORMATION SYSTEM BACKUP

Number
CP-09

Family
Contingency Planning

Name
INFORMATION SYSTEM BACKUP

Baseline
Low; Moderate; High

Description
The organization:

a. Conducts backups of user-level information contained in the information system on a daily basis or more frequently if required;
b. Conducts backups of system-level information contained in the information system on a daily basis or more frequently if required;
c. Conducts backups of information system documentation including security-related documentation; and
d. Protects the confidentiality, integrity, and availability of backup information at storage locations.

NIST Guidance
System-level information includes, for example, system-state information, operating system and application software, and licenses. User-level information includes any information other than system-level information. Mechanisms employed by organizations to protect the integrity of information system backups include, for example, digital signatures and cryptographic hashes. Protection of system backup information while in transit is beyond the scope of this control. Information system backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information.

Related controls: CP-2, CP-6, MP-4, MP-5, SC-13.

References: NIST Special Publication 800-34.

DHSS Guidance
A. This sub control is met if you utilize your personal network shares.

B. This sub control is met if your system is located in the DHSS data center. If not you'll have to get with your technical contacts to understand if you are meeting this requirement.

C. See A and B.

D. See A and B.

CP-10: INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Number
CP-10

Family
Contingency Planning

Name
INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Baseline
Low; Moderate; High

Description
The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

NIST Guidance
Recovery is executing information system contingency plan activities to restore organizational missions/business functions. Reconstitution takes place following recovery and includes activities for returning organizational information systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities, recovery point/time and reconstitution objectives, and established organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of any interim information system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored information system capabilities, reestablishment of continuous monitoring activities, potential information system reauthorizations, and activities to prepare the systems against future disruptions, compromises, or failures. Recovery/reconstitution capabilities employed by organizations can include both automated mechanisms and manual procedures.

Related controls: CA-2, CA-6, CA-7, CP-2, CP-6, CP-7, CP-9, SC-24.

References: Federal Continuity Directive 1; NIST Special Publication 800-34.

DHSS Guidance
If you use the DHSS data centers then this control is managed for you by DHSS networking. If you host servers in your local offices, or utilize a third party then you'll need to contact them to understand if you meet the control requirements above.

IA-02: IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Number
IA-02

Family
Identification and Authentication

Name
IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Baseline
Low; Moderate; High

Description
The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

NIST Guidance
Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., contractors, guest researchers). This control applies to all accesses other than: (i) accesses that are explicitly identified and documented in AC-14; and (ii) accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity. Organizations employ passwords, tokens, or biometrics to authenticate user identities, or in the case multifactor authentication, or some combination thereof. Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks (e.g., the Internet). Internal networks include local area networks and wide area networks. In addition, the use of encrypted virtual private networks (VPNs) for network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network.

Organizations can satisfy the identification and authentication requirements in this control by complying with the requirements in Homeland Security Presidential Directive 12 consistent with the specific organizational implementation plans. Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification

number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD common access card. In addition to identifying and authenticating users at the information system level (i.e., at logon), organizations also employ identification and authentication mechanisms at the application level, when necessary, to provide increased information security. Identification and authentication requirements for other than organizational users are described in IA-8.

Related controls: AC-2, AC-3, AC-14, AC-17, AC-18, IA-4, IA-5, IA-8.

References: HSPD 12; OMB Memoranda 04-04, 06-16, 11-11; FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov.

DHSS Guidance

Generally an Authenticator is a user name and a password. HIPAA requires that everyone who interacts with a system which contains confidential information must have a username and a password. You may do this through Active Directory or through an in-application User creation system.

If you use the DHSS data centers then this control is managed for you by DHSS networking. If you host servers in your local offices, or utilize a third party then you'll need to contact them to understand if you meet the control requirements above.

IA-03: DEVICE IDENTIFICATION AND AUTHENTICATION

Number
IA-03

Family
Identification and Authentication

Name
DEVICE IDENTIFICATION AND AUTHENTICATION

Baseline
Moderate; High

Description
The information system uniquely identifies and authenticates network devices before establishing a high risk network connection.

NIST Guidance
Organizational devices requiring unique device-to-device identification and authentication may be defined by type, by device, or by a combination of type/device. Information systems typically use either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify/authenticate devices on local and/or wide area networks. Organizations determine the required strength of authentication mechanisms by the security categories of information systems. Because of the challenges of applying this control on large scale, organizations are encouraged to only apply the control to those limited number (and type) of devices that truly need to support this capability.

Related controls: AC-17, AC-18, AC-19, CA-3, IA-4, IA-5.

References: None.

DHSS Guidance
We do uniquely identify department computers in the DHSS, however we lack technical controls to make sure this control is complied with.

IA-04: IDENTIFIER MANAGEMENT

Number
IA-04

Family
Identification and Authentication

Name
IDENTIFIER MANAGEMENT

Baseline
Low; Moderate; High

Description
The organization manages information system identifiers by:

a. Receiving authorization from Information Owner or Security Designee to assign an individual, group, role, or device identifier;
b. Selecting an identifier that identifies an individual, group, role, or device;
c. Assigning the identifier to the intended individual, group, role, or device;
d. Preventing reuse of identifiers for at least three (3) years after all previous access authorizations are removed from the system, including all file and other resource accesses for that identifier; and
e. Disabling the identifier after ninety (90) days or less of inactivity.

NIST Guidance
Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). Typically, individual identifiers are the user names of the information system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. This control also addresses individual identifiers not necessarily associated with information system accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to information systems). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.

Related controls: AC-2, IA-2, IA-3, IA-5, IA-8, SC-37.

References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78.

DHSS Guidance

If you're using DHSS Active Directory to manage your users then, this control is managed for you by DHSS networking. If you utilize custom application users ID's, or utilize a third party then you'll need to contact them to understand if you meet the control requirements above.

IA-05: AUTHENTICATOR MANAGEMENT

Number
IA-05

Family
Identification and Authentication

Name
AUTHENTICATOR MANAGEMENT

Baseline
Low; Moderate; High

Description
The organization manages information system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
b. Establishing initial authenticator content for authenticators defined by the organization;
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
e. Changing default content of authenticators prior to information system installation;
f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
g. Changing/refreshing authenticators Passwords: ninety (90) days (Users / Privileged Users / Services); Public Certificates: no longer than three (3) years; Internal Certificates: as determined by Information Owner;
h. Protecting authenticator content from unauthorized disclosure and modification;
i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
j. Changing authenticators for group/role accounts when membership to those accounts changes.

NIST Guidance
Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). In many cases, developers ship information system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored within organizational information systems (e.g., passwords stored in hashed or encrypted formats, files

containing encrypted or hashed passwords accessible with administrator privileges). Information systems support individual authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords.

Related controls: AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS-5, PS-6, SC-12, SC-13, SC-17, SC-28.

References: OMB Memoranda 04-04, 11-11; FIPS Publication 201; NIST Special Publications 800-73, 800-63, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov.

DHSS Guidance

If you're using DHSS Active Directory to manage your users, then this control is managed for you by DHSS networking. If you utilize custom application users IDs, or utilize a third party, then you'll need to contact them to understand if you meet the control requirements above. This is an excellent control to seek guidance from the DSO if you are confused about its details.

IA-06: AUTHENTICATOR FEEDBACK

Number
IA-06

Family
Identification and Authentication

Name
AUTHENTICATOR FEEDBACK

Baseline
Low; Moderate; High

Description
The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

NIST Guidance
The feedback from information systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of information systems or system components, for example, desktops/notebooks with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with 2-4 inch screens, this threat may be less significant, and may need to be balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring the feedback of authentication information includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it.

Related control: PE-18.

References: None.

DHSS Guidance
When users login to your system, is that connection protected? Is the password obscured on the screen? Is the connection encrypted? These are the kinds of questions that need to be answered. If you're using DHSS Active Directory to manage your users then, some of this control is managed for you by DHSS networking. If you utilize custom application users ID's, or utilize a third party then you'll need to contact them to understand if you meet the control requirements above.

IR-01: INCIDENT RESPONSE POLICY AND PROCEDURES

Number
IR-01

Family
Incident Response

Name
INCIDENT RESPONSE POLICY AND PROCEDURES

Baseline
Low; Moderate; High

Description
The organization:

a. Develops, documents, and disseminates to applicable personnel:
   1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and
b. Reviews and updates the current:
   1. Incident response policy within every three hundred sixty-five (365) days; and
   2. Incident response procedures within every three hundred sixty-five (365) days.

NIST Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IR family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Related control: PM-9.

References: NIST Special Publications 800-12, 800-61, 800-83, 800-100.

DHSS Guidance

IR-02: INCIDENT RESPONSE TRAINING

Number
IR-02

Family
Incident Response

Name
INCIDENT RESPONSE TRAINING

Baseline
Low; Moderate; High

Description
The organization provides incident response training to information system users consistent with assigned roles and responsibilities:

a. Within ninety (90) days of assuming an incident response role or responsibility;
b. When required by information system changes; and
c. Within every three hundred sixty-five (365) days thereafter.

NIST Guidance
Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources.

Related controls: AT-3, CP-3, IR-8.

References: NIST Special Publications 800-16, 800-50.

DHSS Guidance
Incidents mentioned in this section and others are events that occur which cause some kind of harm to the system or its data. It might be a hacker illicitly gaining access to confidential information, a database becoming corrupted due to a patching update, or a webpage going down because of some routine failure.

Historically DHSS has not done a very good job of meeting this control, so if this is risk assumption for your division you're in good company.

As an aspirational goal this is where you want to be, performing some kind of incident response training once a year. If you haven't completed this training, and your system is located in the DHSS data center, you're probably okay, because the DHSS regularly handles incidents and has a robust incident handling procedure. However DHSS relies on people on the ground to be aware of who to notify when unexpected events do occur.

If your system is partially located outside the DHSS, or housed inside your division you'll need to give real thought as to what you should do when the unexpected happens, and how you will train division personnel in what they are supposed to do. In the event the unexpected happens, people who have no training will not perform optimally and this may cost your division in the long run.

IR-03: INCIDENT RESPONSE TESTING

Number
IR-03

Family
Incident Response

Name
INCIDENT RESPONSE TESTING

Baseline
Moderate; High

Description
The organization tests the incident response capability for the information system within every three hundred sixty-five (365) days using NIST SP 800-61 to determine the incident response effectiveness and documents the results.

NIST Guidance
Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response.

Related controls: CP-4, IR-8.

References: NIST Special Publications 800-84, 800-115.

DHSS Guidance
Incidents mentioned in this section and others are events that occur which cause some kind of harm to the system or its data. It might be a hacker illicitly gaining access to confidential information, a database becoming corrupted due to a patching update, or a webpage going down because of some routine failure.

Historically DHSS has not done a very good job of meeting this control, so if this is risk assumption for your division you're in good company.

As an aspirational goal this is where you want to be, performing some kind of practice incident once a year. If you haven't completed this exercise, and your system is located in the DHSS data center, you're probably okay, because the DHSS regularly handles incidents and has a robust incident handling procedure. However DHSS

relies on people on the ground to make good choices and notify the correct persons when unexpected events do occur.

If your system is partially located outside the DHSS, or housed inside your division you'll need to give real thought as to what you should do when the unexpected happens. A little practice can go a long way to ensure optimal results when the unexpected happens.

IR-04: INCIDENT HANDLING

Number
IR-04

Family
Incident Response

Name
INCIDENT HANDLING

Baseline
Low; Moderate; High

Description
The organization:

a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
b. Coordinates incident handling activities with contingency planning activities; and
c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

NIST Guidance
Organizations recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and information systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function).

Related controls: AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

References: Executive Order 13587; NIST Special Publication 800-61.

DHSS Guidance
Section A and B are handled by the DSO. However your department should be minimally aware of sections A and B, as well as use information from the DSO to incorporate into your own training and exercises.

If you work with a partner outside of the DHSS then you will need to ensure they are in compliance with this control.

IR-05: INCIDENT MONITORING

Number
IR-05

Family
Incident Response

Name
INCIDENT MONITORING

Baseline
Low; Moderate; High

Description
The organization tracks and documents information system security incidents.

NIST Guidance
Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Related controls: AU-6, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

References: NIST Special Publication 800-61.

DHSS Guidance
This control is managed by the DSO. However your division should be minimally aware incidents which affect you.

If you work with a partner outside of the DHSS then you will need to ensure they are in compliance with this control.

IR-06: INCIDENT REPORTING

Number
IR-06

Family
Incident Response

Name
INCIDENT REPORTING

Baseline
Low; Moderate; High

Description
The organization:

a. Requires personnel to report suspected security incidents to the organizational incident response capability within an expeditious time period; and
b. Reports security incident information to the employee's supervisor and the Department Chief Security Officer.

NIST Guidance
The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling.

Related controls: IR-4, IR-5, IR-8.

References: NIST Special Publication 800-61: Web: www.us-cert.gov.

DHSS Guidance
This control is a critical requirement. When things go wrong who do your users contact? Do they know they need to contact someone?

If you work with a partner outside of the DHSS then you will need to ensure they are in compliance with this control.

IR-07: INCIDENT RESPONSE ASSISTANCE

Number
IR-07

Family
Incident Response

Name
INCIDENT RESPONSE ASSISTANCE

Baseline
Low; Moderate; High

Description
The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

NIST Guidance
Incident response support resources provided by organizations include, for example, help desks, assistance groups, and access to forensics services, when required.

Related controls: AT-2, IR-4, IR-6, IR-8, SA-9.

References: None.

DHSS Guidance
DHSS DSO fulfills this role within our organization. If you have business associates, or other 3rd parties whom are integral to your application you'll need to make sure they have their own resources.

MA-01: SYSTEM MAINTENANCE POLICY AND PROCEDURES

Number
MA-01

Family
Maintenance

Name
SYSTEM MAINTENANCE POLICY AND PROCEDURES

Baseline
Low; Moderate; High

Description
The organization:

a. Develops, documents, and disseminates to applicable personnel:
   1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and
b. Reviews and updates the current:
   1. System maintenance policy within every three hundred sixty-five (365) days; and
   2. System maintenance procedures within every three hundred sixty-five (365) days.

NIST Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Related control: PM-9.

References: NIST Special Publications 800-12, 800-100.

DHSS Guidance

MA-02: CONTROLLED MAINTENANCE

Number
MA-02

Family
Maintenance

Name
CONTROLLED MAINTENANCE

Baseline
Low; Moderate; High

Description
The organization:

a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
c. Requires that the applicable Information Owner (or an official designated in the applicable security plan) explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
f. Includes defined maintenance-related information (defined in the applicable security plan) in organizational maintenance records.

NIST Guidance
This control addresses the information security aspects of the information system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement). System maintenance also includes those components not directly associated with information processing and/or data/information retention such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes, for example: (i) date and time of maintenance; (ii) name of individuals or group performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) information system components/equipment removed or replaced (including identification numbers, if applicable). The level of detail included in maintenance records can be informed by the security categories of

organizational information systems. Organizations consider supply chain issues associated with replacement components for information systems.

Related controls: CM-3, CM-4, MA-4, MP-6, PE-16, SA-12, SI-2.

References: None.

DHSS Guidance

This control is in reference to physical systems like servers, network systems, and hard drives. There are a number of different state holders in the State of Alaska Environment. If your system is inside the DHSS data center then network services and the enterprise technology services takes care of this control for you, and you'll need to get their input for this control. If your system is managed wholly or in part by a third party then you'll need to get this information from them.

MA-05: MAINTENANCE PERSONNEL

Number
MA-05

Family
Maintenance

Name
MAINTENANCE PERSONNEL

Baseline
Low; Moderate; High

Description
The organization:

a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and
c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

NIST Guidance
This control applies to individuals performing hardware or software maintenance on organizational information systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Technical competence of supervising individuals relates to the maintenance performed on the information systems while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, systems integrators, and consultants, may require privileged access to organizational information systems, for example, when required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods.

Related controls: AC-2, IA-8, MP-2, PE-2, PE-3, PE-4, RA-3.

References: None.

DHSS Guidance

This control is in reference to physical systems like servers, network systems, and hard drives. There are a number of different state holders in the State of Alaska Environment. If your system is inside the DHSS data center then network services and the enterprise technology services takes care of this control for you, and you'll need to get their input for this control. If your system is managed wholly or in part by a third party then you'll need to get this information from them.

MP-01: MEDIA PROTECTION POLICY AND PROCEDURES

Number
MP-01

Family
Media Protection

Name
MEDIA PROTECTION POLICY AND PROCEDURES

Baseline
Low; Moderate; High

Description
The organization:

a. Develops, documents, and disseminates to applicable personnel:
   1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and
b. Reviews and updates the current:
   1. Media protection policy within every three hundred sixty-five (365) days; and
   2. Media protection procedures within every three hundred sixty-five (365) days.

NIST Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Related control: PM-9.

References: NIST Special Publications 800-12, 800-100.

DHSS Guidance

MP-02: MEDIA ACCESS

Number
MP-02

Family
Media Protection

Name
MEDIA ACCESS

Baseline
Moderate; High

Description
The organization restricts access to classified data including but not limited to: PII, ePHI, FTI, CJI, etc. to authorized individuals.

NIST Guidance
Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team.

Related controls: AC-3, IA-2, MP-4, PE-2, PE-3, PL-2.

References: FIPS Publication 199; NIST Special Publication 800-111.

DHSS Guidance
This control is about media of all types, hard drives (and electronic information), email, flash drives, paper records, and even microfiche. A coherent plan on who gets access (meaning the ability to walk around and touch, or open from a network folder) to what and when should already be part of your plan for access control.

MP-04: MEDIA STORAGE

Number
MP-04

Family
Media Protection

Name
MEDIA STORAGE

Baseline
Moderate; High

Description
The organization:

a. Physically controls and securely stores all unencrypted media within secure areas; and
b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

NIST Guidance
Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Physically controlling information system media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. The type of media storage is commensurate with the security category and/or classification of the information residing on the media. Controlled areas are areas for which organizations provide sufficient physical and procedural safeguards to meet the requirements established for protecting information and/or information systems. For media containing information determined by organizations to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on organizations or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls provide adequate protection.

Related controls: CP-6, CP-9, MP-2, MP-7, PE-3.

References: FIPS Publication 199; NIST Special Publications 800-56, 800-57, 800-111.

DHSS Guidance

DHSS meets this control in our data centers with locked doors, video cameras, and sign in sheets. DHSS additionally encrypts all other media by policy. If you utilize third party services, business partners, or host on own devices you'll need to explain how you meet this control.

MP-05: MEDIA TRANSPORT

Number
MP-05

Family
Media Protection

Name
MEDIA TRANSPORT

Baseline
Moderate; High

Description
The organization:

a. Protects and controls unencrypted digital and non-digital media containing sensitive information, such as Personally Identifiable Information (PII), during transport outside of controlled areas using tamper-evident packaging, and (i) if hand carried, using securable container (e.g., locked briefcase) via authorized personnel, or (ii) if shipped, trackable with receipt by commercial carrier;
b. Maintains accountability for information system media during transport outside of controlled areas;
c. Documents activities associated with the transport of information system media; and
d. Restricts the activities associated with the transport of information system media to authorized personnel.

NIST Guidance
Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers), that are transported outside of controlled areas. Controlled areas are areas or spaces for which organizations provide sufficient physical and/or procedural safeguards to meet the requirements established for protecting information and/or information systems.

Physical and technical safeguards for media are commensurate with the security category or classification of the information residing on the media. Safeguards to protect media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service).

Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and/or obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with organizational assessments of risk to include the flexibility to define different record-keeping methods for the different types of media transport as part of an overall system of transport-related records.

Related controls: AC-19, CP-9, MP-3, MP-4, RA-3, SC-8, SC-13, SC-28.

References: FIPS Publication 199; NIST Special Publication 800-60.

DHSS Guidance

This control can be thought of as having two main parts, digital and physical.

For transporting large volumes of physical media (papers, microfiche, etc), it is important to have a plan for ensuring confidentiality in transit.

For transporting digital media, encryption is key. You'll need to develop a plan for either encrypting drives or other physical containers of data, or encryption in transit. The DHSS DSO can assist you in your endeavors.

If you're working with 3rd parties you'll need to ensure that they have a plan for encrypting media in transit.

MP-06: MEDIA SANITIZATION

Number
MP-06

Family
Media Protection

Name
MEDIA SANITIZATION

Baseline
Low; Moderate; High

Description
The organization:

a. Sanitizes both digital and non-digital information system media prior to disposal, release out of organizational control, or release for reuse using State and Department standard sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies; and
b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

NIST Guidance
This control applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media containing classified information.

Related controls: MA-2, MA-4, RA-3, SC-4.

References: FIPS Publication 199; NIST Special Publications 800-60, 800-88; Web: www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml.

DHSS Guidance

Computer hard drives, DVDs, thumb drives, and other storage media need to be securely erased before being thrown out (or otherwise disposed of, released, or re-used). This not only applies to computers, but also to devices such as cell phones, printers, and copy machines. It even applies to non-digital media such as paper documents, photographs, tape recordings, etc. Refer to State of Alaska policy ISP-143 for details on secure disposal requirements. Currently, a DoD or NIST 800-88 compliant secure erase or physical destruction is required for digital media, and cross-cut shredding or burning is required for printed media.

Your information system is hosted on computers that contain storage media of one form or another. By their nature, these storage media need to be replaced from time to time — usually they either wear out on their own or get replaced with newer technology during a hardware upgrade. Additionally, almost all information systems have data backups that are stored to tape or disk media (often at offsite locations), as well as input/output devices such as workstations, printers, fax servers, etc. Talk to those who maintain these systems and devices to make sure that their media disposal processes for digital and non-digital media meet or exceed the State of Alaska ISP-143 requirements. Provide a short summary and include any supporting information on how the requirements are met.

Example: System X is hosted for us by ACME Industries. According to the documentation that ACME has provided us (see attached), they are FedRAMP Moderate certified and use a NIST 800-88 compliant media sanitization process for all digital media that is taken out of service or repurposed. Customer data is never printed or otherwise stored in non-digital form.

PE-01: PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Number
PE-01

Family
Physical and Environmental Protection

Name
PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Baseline
Low; Moderate; High

Description
The organization:

a. Develops, documents, and disseminates to applicable personnel:
   1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and
b. Reviews and updates the current:
   1. Physical and environmental protection policy within every three hundred sixty-five (365) days; and
   2. Physical and environmental protection procedures within every three hundred sixty-five (365) days.

NIST Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PE family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Related control: PM-9.

References: NIST Special Publications 800-12, 800-100.

DHSS Guidance

PE-02: PHYSICAL ACCESS AUTHORIZATIONS

Number
PE-02

Family
Physical and Environmental Protection

Name
PHYSICAL ACCESS AUTHORIZATIONS

Baseline
Low; Moderate; High

Description
The organization:

a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
b. Issues authorization credentials for facility access;
c. Reviews the access list detailing authorized facility access by individuals at least once every one hundred eighty (180) days; and
d. Removes individuals from the facility access list when access is no longer required.

NIST Guidance
This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Authorization credentials include, for example, badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed (including level of forge-proof badges, smart cards, or identification cards) consistent with federal standards, policies, and procedures. This control only applies to areas within facilities that have not been designated as publicly accessible.

Related controls: PE-3, PE-4, PS-3.

References: None.

DHSS Guidance
Physical access to the data centers where information systems reside must be very carefully restricted to authorized personnel. The organization needs to keep track of everyone who is allowed to access the facility, manage authorization credentials (badges, key cards, etc), and review the access list on a regular basis, making sure that the list only includes those who currently require access.

Check with those who host your information system to make sure that this is being done and provide a summary of how these authorization requirements are being met.

Example: System X is hosted for us by ACME Industries. Access to their data center is restricted to certain employees and these employees are issued color coded badges, key cards, and daily passwords to authorize entry. The access list is reviewed every month and updated anytime staff or access requirements change.

PE-03: PHYSICAL ACCESS CONTROL

Number
PE-03

Family
Physical and Environmental Protection

Name
PHYSICAL ACCESS CONTROL

Baseline
Low; Moderate; High

Description
The organization:

a. Enforces physical access authorizations at defined entry/exit points to the facility where the information system resides by;
   1. Verifying individual access authorizations before granting access to the facility; and
   2. Controlling ingress/egress to the facility using physical access devices/or guards;
b. Maintains physical access audit logs for defined entry/exit points to the facility;
c. Provides security safeguards to control access to areas within the facility officially designated as publicly accessible;
d. Escorts visitors and monitors visitor activity;
e. Secures keys, combinations, and other physical access devices;
f. Inventories physical access devices every three hundred sixty-five (365) days; and
g. Changes combinations and keys within every three hundred sixty-five (365) days and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

NIST Guidance
This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas. Physical access control systems comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The Federal Identity, Credential, and Access Management Program provides implementation guidance for identity, credential, and access management capabilities for physical access control systems. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when

such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices.

Related controls: AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3.

References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78, 800-116; ICD 704, 705; DoDI 5200.39; Personal Identity Verification (PIV) in Enterprise Physical Access Control System (E-PACS); Web: idmanagement.gov, fips201ep.cio.gov.

DHSS Guidance

Once you figure out who is allowed in the data center (see PE-02), the next step is making sure they're the only ones who can get in. This is done by checking authorization at all entry and exit points and physically controlling access based on the results of the check. There are a variety of ways to achieve this ranging from placing standard locks on doors and issuing keys to authorized personnel, to posting guards at access points to confirm identities and verify authorization. This control includes additional safeguards such as maintaining access logs, escorting visitors, and managing keys and other access devices.

Check with those who host your information system to make sure that this is being done and provide a summary of how these access control requirements are being met.

Example: System X is hosted for us by ACME Industries. Access to their data center is controlled through the use of keycard locks on doors, combined with a daily PIN code. Their electronic access system automatically logs all access to the facility. Employees sign an agreement saying they will keep their keycard and PIN secure at all times and will report immediately if lost or stolen. Card readers and keypads are designed and installed in way to make them very difficult to tamper with. Keycards are immediately revoked when lost, stolen, employee leaves, or access is otherwise not needed. All visitor access is escorted, monitored, and logged. Security devices are inventoried every six months.

PE-04: ACCESS CONTROL FOR TRANSMISSION MEDIUM

Number
PE-04

Family
Physical and Environmental Protection

Name
ACCESS CONTROL FOR TRANSMISSION MEDIUM

Baseline
Moderate; High

Description
The organization controls physical access to information system distribution and transmission lines within organizational facilities using defined security safeguards.

NIST Guidance
Physical security safeguards applied to information system distribution and transmission lines help to prevent accidental damage, disruption, and physical tampering. In addition, physical safeguards may be necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Security safeguards to control physical access to system distribution and transmission lines include, for example: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.

Related controls: MP-2, MP-4, PE-2, PE-3, PE-5, SC-7, SC-8.

References: NSTISSI No. 7003.

DHSS Guidance
The cables and wires that computers send information over need to be secured in order to avoid tampering and eavesdropping. This not only includes the cable connecting the computer to the wall jack, but also the wall jacks themselves, as well as the building's internal wiring and conduits, wiring closets, and cable trays. Unused wall jacks are an often overlooked security issue since they can be used to give an unauthorized person access to the network. Generally, anything that isn't behind a locked door should have some kind physical protection or tamper-proofing in place to prevent unauthorized access.

Check with those who host your information system to make sure that this is being done and provide a summary of how these access control requirements are being met.

System X is hosted for us by ACME Industries. According to the documentation that ACME has provided us (see attached), this is done as part of their FedRAMP Moderate certification.

PE-05: ACCESS CONTROL FOR OUTPUT DEVICES

Number
PE-05

Family
Physical and Environmental Protection

Name
ACCESS CONTROL FOR OUTPUT DEVICES

Baseline
Moderate; High

Description
The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

NIST Guidance
Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can be monitored by organizational personnel. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices.

Related controls: PE-2, PE-3, PE-4, PE-18.

References: None.

DHSS Guidance
Output devices include things like printers, fax machines, DVD burners, and computer monitors. These need to be secured to prevent unauthorized acquisition or viewing of output. This usually means keeping the devices and media behind locked doors, only accessible to authorized personnel. Additional safeguards such as privacy screens for monitors are often required to defend against prying eyes.

Check with those who host your information system as well as persons within your organization who use the system to make sure that all output devices are properly secured and processes are in place to protect the devices, media, and output. Provide a summary of the output devices and safeguards as well as any supporting documentation.

System X is hosted for us by ACME Industries. As outlined in their Service Level Agreement (attached), ACME never views, prints, exports, or otherwise outputs our sensitive data. The twenty end users in our organization

enter and view sensitive data only from their protected workstations. All paper outputs are sent to a single enterprise printer, which is in a locked closet only accessible to section employees.

PE-06: MONITORING PHYSICAL ACCESS

Number
PE-06

Family
Physical and Environmental Protection

Name
MONITORING PHYSICAL ACCESS

Baseline
Low; Moderate; High

Description
The organization:

a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
b. Reviews physical access logs at least monthly and upon occurrence of security incidents involving physical security; and
c. Coordinates results of reviews and investigations with the organizational incident response capability.

NIST Guidance
Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses.

Related controls: CA-7, IR-4, IR-8.

References: None.

DHSS Guidance
Physical access to the data center where the application is hosted needs to be monitored, logs should be reviewed at least monthly, and physical security incidents need to be investigated and responded to in a documented and consistent manner.

Check with those who host your information system to make sure that their data center(s) provide this level of physical monitoring, review, and incident response. Provide a summary of how these control requirements are being met.

System X is hosted for us by ACME Industries. Their secure data center is monitored through keycard access logs and video surveillance devices. Video is reviewed daily and keycard logs are reviewed weekly. All anomalies are

investigated and documented, including reviews of all relevant logs. Customers are alerted immediately if physical security has been compromised.

PE-08: VISITOR ACCESS RECORDS

Number
PE-08

Family
Physical and Environmental Protection

Name
VISITOR ACCESS RECORDS

Baseline
Low; Moderate; High

Description
The organization:

a. Maintains visitor access records to the facility where the information system resides for two (2) years; and
b. Reviews visitor access records at least monthly.

NIST Guidance
Visitor access records include, for example, names and organizations of persons visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purposes of visits, and names and organizations of persons visited. Visitor access records are not required for publicly accessible areas.

References: None.

DHSS Guidance
Visitors to secure data centers are persons who are not normally authorized to access the facility. Examples would include executives being given a tour, fire/building inspectors, and HVAC maintenance personnel. As described in PE-03, visitors must be escorted and their access must be logged. The additional requirements of PE-08 are that the logs must be retained for two years and reviewed at least monthly.

Check with those who host your information system to make sure that visitor logs are kept for their data center(s) and reviewed in a way that meets the requirements of this control.

System X is hosted for us by ACME Industries. This control is met as part of their FedRAMP Moderate certification (attached).

PE-17: ALTERNATE WORK SITE

Number
PE-17

Family
Physical and Environmental Protection

Name
ALTERNATE WORK SITE

Baseline
Moderate; High

Description
The organization:

a. Employs appropriate security controls at alternate work sites;
b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and
c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

NIST Guidance
Alternate work sites may include, for example, government facilities or private residences of employees. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. Organizations may define different sets of security controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites. This control supports the contingency planning activities of organizations and the federal telework initiative.

Related controls: AC-17, CP-7.

References: NIST Special Publication 800-46.

DHSS Guidance
As part of an organization-wide contingency plan, alternative worksites are defined in order to provide employees with a place to work in the event that their usual place of business is unavailable. Due to cost and availability constraints, this often means employees have to work from home for a period of time. The organization needs to make sure that appropriate security safeguards will still be in place at these alternate work sites. The organization will need to assess the safeguards to make sure they are working as expected and additionally provide a way for employees to communicate security issues remotely back to organization security personnel.

If your organization has an operational contingency plan that includes alternate workspaces, check to make sure that provision has been made for appropriate security safeguards, assessment of the safeguards, and communication of security issues from/to alternate locations.

Our organization has not defined alternate worksites. Control is N/A.

PE-18: LOCATION OF INFORMATION SYSTEM COMPONENTS

Number
PE-18

Family
Physical and Environmental Protection

Name
LOCATION OF INFORMATION SYSTEM COMPONENTS

Baseline
Moderate; High

Description
The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards, and to minimize the opportunity for unauthorized access.

NIST Guidance
Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. In addition, organizations consider the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to information systems and therefore increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones).

Related controls: CP-2, PE-19, RA-3.

References: None.

DHSS Guidance
Data centers need to be located and designed properly to reduce risk from physical and environmental hazards. Examples of this would include locating the data center on the ground floor or basement of a building and not along an outside wall or publicly accessible area, avoiding construction of data centers in seismically active areas (like Anchorage), and laying out the data center to minimize damage from potential HVAC, UPS, transformer, fire protection, and other failures.

Check with those who host your information system to ensure that their data center has been designed with these considerations in mind and provide some documentation to support it.

System X is hosted for us by ACME Industries. This control is met as part of their FedRAMP Moderate certification (attached).

PL-01: SECURITY PLANNING POLICY AND PROCEDURES

Number
PL-01

Family
Planning

Name
SECURITY PLANNING POLICY AND PROCEDURES

Baseline
Low; Moderate; High

Description
The organization:

a. Develops, documents, and disseminates to applicable personnel:
   1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and
b. Reviews and updates the current:
   1. Security planning policy within every three hundred sixty-five (365) days; and
   2. Security planning procedures within every three hundred sixty-five (365) days.

NIST Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PL family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Related control: PM-9.

References: NIST Special Publications 800-12, 800-18, 800-100.

DHSS Guidance

PS-01: PERSONNEL SECURITY POLICY AND PROCEDURES

Number
PS-01

Family
Personnel Security

Name
PERSONNEL SECURITY POLICY AND PROCEDURES

Baseline
Low; Moderate; High

Description
The organization:

a. Develops, documents, and disseminates to applicable personnel:
   1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and
b. Reviews and updates the current:
   1. Personnel security policy within every three hundred sixty-five (365) days; and
   2. Personnel security procedures within every three hundred sixty-five (365) days.

NIST Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PS family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Related control: PM-9.

References: NIST Special Publications 800-12, 800-100.

DHSS Guidance

PS-02: POSITION RISK DESIGNATION

Number
PS-02

Family
Personnel Security

Name
POSITION RISK DESIGNATION

Baseline
Low; Moderate; High

Description
The organization:

a. Assigns a risk designation to all organizational positions;
b. Establishes screening criteria for individuals filling those positions; and
c. Reviews and updates position risk designations within every three hundred sixty-five (365) days.

NIST Guidance
Position risk designations reflect Office of Personnel Management policy and guidance. Risk designations can guide and inform the types of authorizations individuals receive when accessing organizational information and information systems. Position screening criteria include explicit information security role appointment requirements (e.g., training, security clearances).

Related controls: AT-3, PL-2, PS-3.

References: 5 C.F.R. 731.106(a).

DHSS Guidance
To implement this control, organizations perform a risk assessment for all positions and integrate the resulting risk designation into their HR processes. This generally results in additional background checks and other screening being required for persons hired into higher risk positions. Currently, neither the State of Alaska nor DHSS track risk as part of their organization-wide job classification processes, so it may be necessary to implement this control at the division, section, or group level. This control may be at least partially fulfilled by some divisions that require background checks on employees working with sensitive information or regularly dealing with vulnerable persons. These risk designations, requirements, and processes need to be documented and disseminated to hiring managers and HR staff. They also need to be reviewed regularly and updated whenever positions or job classes change.

Talk to hiring managers within your division or section to find out if the risk designation, screening, and review requirements of this control are appropriately implemented where you work. Provide a summary of the processes and include supporting policies, manuals, and other documentation.

Group Z has prepared a hiring manual (attached) and related training material which is provided to all supervisors in the group. The manual contains a list of high risk PCNs that require the applicant to pass a background check before being hired. The list is reviewed every six months and updated whenever duties, positions, or job classifications change.

PS-03: PERSONNEL SCREENING

Number
PS-03

Family
Personnel Security

Name
PERSONNEL SCREENING

Baseline
Low; Moderate; High

Description
The organization:

a. Screens individuals prior to authorizing access to the information system; and
b. Rescreens individuals according to the criticality/sensitivity risk designation of the position, on a periodic basis and at least every three (3) years.

NIST Guidance
Personnel screening and rescreening activities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions. Organizations may define different rescreening conditions and frequencies for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems.

Related controls: AC-2, IA-4, PE-2, PS-2.

References: 5 C.F.R. 731.106; FIPS Publications 199, 201; NIST Special Publications 800-60, 800-73, 800-76, 800-78; ICD 704.

DHSS Guidance
This control requires screening of everyone who uses the information system, but leaves the level of screening open for the organization to determine based on the level of risk. For some lower security systems, it may be sufficient to require someone to be a DHSS employee with a signed usage agreement on file. For higher risk systems, the person may need to pass a background check before access is granted. It is up to the organization to determine what level of screening is appropriate based on the level of risk associated with the use of the system. The basic question is: How much damage could they do? Additionally, this control requires the screening process to be repeated every three years or sooner.

Decide what level of risk is involved with use of your application. Decide what level of screening is appropriate to mitigate the risk, and document the decision. Create and document screening procedures for the application to make sure that all users are screened before access and rescreened every three years or sooner. Provide a summary and include relevant documentation, checklists, and forms.

Background checks are performed before granting someone access to the application and every year thereafter. Only employees passing the check are allowed access. Attached are the procedure document and application form.

PS-04: PERSONNEL TERMINATION

Number
PS-04

Family
Personnel Security

Name
PERSONNEL TERMINATION

Baseline
Low; Moderate; High

Description
The organization, upon termination of individual employment:

a. Disables information system access within a time period ending prior to or during the employee termination process, or prior to notification if employee is terminated for cause;
b. Terminates/revokes any authenticators/credentials associated with the individual;
c. Conducts exit interviews that include a discussion of non-disclosure of information security and privacy information;
d. Retrieves all security-related organizational information system-related property;
e. Retains access to organizational information and information systems formerly controlled by terminated individual; and
f. Notifies applicable stakeholders within one (1) business day.

NIST Guidance
Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and lack of availability of supervisors. Exit interviews are important for individuals with security clearances. Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, organizations consider disabling the information system accounts of individuals that are being terminated prior to the individuals being notified.

Related controls: AC-2, IA-4, PE-2, PS-5, PS-6.

References: None.

DHSS Guidance

It's important that an organization have good employee termination procedures in place to reduce risk and make sure nothing is overlooked. It is critical that the terminated employee can no longer access computers, applications, protected information, and other resources; but it is also important that the employer will still maintain access to these things after the employee leaves. When the employee termination is involuntary on the part of the employee, access should be revoked before the employee is informed of the decision. The control mentions that all authenticators and credentials should be revoked (or retrieved). These would include things like keys, badges, access cards, soft tokens, door combinations, and passwords — anything used for access to protected systems, information, and areas. This would also be the appropriate time to retrieve other organization-owned property, especially if it is security-related (laptops, cell phones, thumb drives, etc.). The control also mentions exit interviews and a discussion of privacy and non-disclosure, as well as notification requirements.

Check with your organization's Human Resources group to make sure that their employee termination process meets these requirements. Check with supervisors to make sure that the process is being followed. Summarize the process and reference or attach relevant policies, procedures, forms, and checklists.

Our organization uses the attached separation checklist and form for employee terminations. It is the supervisor's responsibility to make sure that everything is completed before submitting the signed form to HR. The form includes checkboxes for deactivation of all accounts, passwords, and other authenticators; retrieval of all company property including badges and key cards, and transfer of any access codes or specialized knowledge required to perform job duties. Employees are asked to sign the attached non-disclosure agreement. Notification is sent out to organization managers by close of business on the day of termination. Relevant policies and procedures are attached for reference.

PS-05: PERSONNEL TRANSFER

Number
PS-05

Family
Personnel Security

Name
PERSONNEL TRANSFER

Baseline
Low; Moderate; High

Description
The organization:

a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
b. Initiates the re-issuing of appropriate information system-related property (e.g., keys, identification cards, and building passes), notification to security management, closing of obsolete accounts and establishing new accounts, and re-evaluation of logical and physical access controls within thirty (30) days;
c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
d. Notifies applicable stakeholders within one (1) business day.

NIST Guidance
This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted. Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing information system accounts and establishing new accounts; (iii) changing information system access authorizations (i.e., privileges); and (iv) providing for access to official records to which individuals had access at previous work locations and in previous information system accounts.

Related controls: AC-2, IA-4, PE-2, PS-4.

References: None.

DHSS Guidance

The definition of transfer used here is a little bit different than how the State of Alaska defines a transfer. As used here, personnel transfer means any time an employee moves from one job position (PCN) into a different position (including promotions). Transfers can occur within the same group or across sections, divisions, or departments. Whenever a transfer happens, it is important that the employee's access to applications, information, resources, and facilities is reviewed and updated as appropriate to the change in duties. It is especially important that any access that is no longer needed in the new position be removed. Refer to control AC-06: Least Privilege for a discussion of why this is so important. It is also common for new access to be added at this time, when needed to perform new job duties. Adding and removing access is done through a variety of ways, and can include changes to group membership, creating/disabling accounts, issuing/collecting keys or keycards, and resetting passwords or PINs. An additional requirement of this control is that applicable personnel be notified of the transfer within one day.

Check to see if your organization is meeting these requirements for all personnel transfers. Provide a short summary of the processes used and any relevant documentation including policies, procedures, checklists, and forms.

Our organization has defined standard procedures for personnel transfers (see attached policy and procedure documents). To summarize the relevant part of the process: Access authorizations are implemented through Active Directory group membership. We have defined access templates for each position in our organization. When an employee transfers to a different position, all access authorizations are initially removed. Then the appropriate access template for the new position is applied. This ensures that each employee is only ever granted access appropriate to their current position. Access templates are reviewed every six month or whenever duties, positions, or access requirements change. Whenever employees change locations, the facilities office is notified and will update keycard access on the day of the change (see attached facilities documentation). All organization managers are notified the same day that transfers have occurred.

PS-06: ACCESS AGREEMENTS

Number
PS-06

Family
Personnel Security

Name
ACCESS AGREEMENTS

Baseline
Low; Moderate; High

Description
The organization:

a. Develops and documents access agreements for organizational information systems;
b. Reviews and updates the access agreements within every three hundred sixty-five (365) days; and
c. Ensures that individuals requiring access to organizational information and information systems:
    1. Sign appropriate access agreements prior to being granted access; and
    2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated.

NIST Guidance
Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational information systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy.

Related control: PL-4, PS-2, PS-3, PS-4, PS-8.

References: None.

DHSS Guidance
Access Agreements can take different forms, but in our case they are usually in the form of a Use or Usage Agreement which users must read and sign before they are allowed to use an application. The agreement should explain roles and responsibilities, outline acceptable and unacceptable use, discuss sanctions and reporting of violations, and remind users of important security and privacy requirements. When HIPAA or other protected data is involved, the principle of minimum necessary access is extremely important, and should be called out in the agreement. It acceptable for these agreements to be included as part of a new account form, provided that

there is still a place for the user to acknowledge and sign that they will follow the agreement. These agreements are important for a variety of reasons including the fulfillment of the department's various security requirements, as well as compliance with HR and other organizational policies and procedures.

If your application does not have a usage agreement, you'll need to create one for it, but of course it's not necessary to re-invent the wheel. Look around for other usage agreements for similar applications in your group, section, or division. Or ask the DSO for a copy of one. You can use these as a starting point, but make sure to review the agreement thoroughly and make appropriate changes as necessary for the specific application.

As part of our onboarding process for new users of this application, everyone must attend our training session and sign the attached usage agreement before they are given access.

PS-07: THIRD-PARTY PERSONNEL SECURITY

Number
PS-07

Family
Personnel Security

Name
THIRD-PARTY PERSONNEL SECURITY

Baseline
Low; Moderate; High

Description
The organization:

a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
b. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
c. Documents personnel security requirements;
d. Requires third-party providers to notify contract administrator of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within fifteen (15) calendar days; and
e. Monitors provider compliance.

NIST Guidance
Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. Organizations explicitly include personnel security requirements in acquisition-related documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by organizations. Notifications of third-party personnel changes ensure appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred or terminated.

Related controls: PS-2, PS-3, PS-4, PS-5, PS-6, SA-9, SA-21.

References: NIST Special Publication 800-35.

DHSS Guidance

When we contract with vendors outside of HSS for services, it is important that the vendor follow personnel security standards similar to those followed by HSS personnel. The main way that we make sure this happens is through the contracts that we have our vendors sign. These contracts should contain language stating that the vendor agrees to follow all State of Alaska and DHSS policies and procedures. Additionally, it is HSS' responsibility to monitor the vendor for compliance with these security standards. This should be done as part of our regular contract monitoring and enforcement activities.

Review the contract for the vendor supporting your application to ensure that these personnel security requirements are met. Talk with the project manager for your project to ensure that monitoring of the vendor's security compliance is being done.

This control is mainly met through the contract that we have with ACME Industries. See section VII of the attached contract. We have weekly status meetings with the vendor where personnel security issues can and have been discussed. Additional monitoring is provided through our VPN and account access approval process.

PS-08: PERSONNEL SANCTIONS

Number
PS-08

Family
Personnel Security

Name
PERSONNEL SANCTIONS

Baseline
Low; Moderate; High

Description
The organization:

a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and
b. Notifies appropriate stakeholders within a reasonable period of time, when applicable, when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

NIST Guidance
Organizational sanctions processes reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for organizations. Organizations consult with the Office of the General Counsel regarding matters of employee sanctions.

Related controls: PL-4, PS-6.

References: None.

DHSS Guidance
This control is implemented at the organizational level by the Department Security Office.

Check with your Department Security Office to make sure they are doing this and have created an organizational authorization package that you can inherit this control from. If not, remind them that security is a team effort, and that a little work on their part can save a lot of work for everyone else.

System X inherits this control from the DHSS Organization authorization package.

RA-01: RISK ASSESSMENT POLICY AND PROCEDURES

Number
RA-01

Family
Risk Assessment

Name
RISK ASSESSMENT POLICY AND PROCEDURES

Baseline
Low; Moderate; High

Description
The organization:

a. Develops, documents, and disseminates to applicable personnel:
   1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and
b. Reviews and updates the current:
   1. Risk assessment policy within every three hundred sixty-five (365) days; and
   2. Risk assessment procedures within every three hundred sixty-five (365) days.

NIST Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the RA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Related control: PM-9.

References: NIST Special Publications 800-12, 800-30, 800-100.

DHSS Guidance

RA-02: SECURITY CATEGORIZATION

Number
RA-02

Family
Risk Assessment

Name
SECURITY CATEGORIZATION

Baseline
Low; Moderate; High

Description
The organization:

a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
c. Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

NIST Guidance
Clearly defined authorization boundaries are a prerequisite for effective security categorization decisions. Security categories describe the potential adverse impacts to organizational operations, organizational assets, and individuals if organizational information and information systems are comprised through a loss of confidentiality, integrity, or availability. Organizations conduct the security categorization process as an organization-wide activity with the involvement of chief information officers, senior information security officers, information system owners, mission/business owners, and information owners/stewards. Organizations also consider the potential adverse impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level adverse impacts. Security categorization processes carried out by organizations facilitate the development of inventories of information assets, and along with CM-8, mappings to specific information system components where information is processed, stored, or transmitted.

Related controls: CM-8, MP-4, RA-3, SC-7.

References: FIPS Publication 199; NIST Special Publications 800-30, 800-39, 800-60.

DHSS Guidance

This is done as part of our Archer authorization process. As one of the first steps in the process, you have to figure out what types of information are present in the application and how sensitive the information is. This must be done first because it will effect which controls are selected later on. Data that is more sensitive will need more controls to keep it safe. Security Categorization is done in the third tab of your Archer authorization package (not coincidentally called "Security Category"). This is the part where you selected all of the information types that are present in your application. Examples of information types are PCI (credit card), PII (Personally Identifiable Information), and ePHI (electronic Protected Health Information). You should have selected all information types present within the system boundary described in the previous, "Boundary" tab. Once this is done, the system will automatically pick a control baseline for your application. A little later in the process, controls will be selected and added to the authorization package according to this baseline. But more importantly for this control, the selected baseline will be reviewed and approved by the DSO as part of the overall approval for this authorization package.

If you're using Archer and have gotten this far, then your application has already been categorized. The DSO will review the categorization after the authorization package is submitted for approval.

As documented in this authorization package, this information system includes Personally Identifiable Information as well as Protected Health Information and has been categorized by Archer as Moderate. This categorization will be reviewed and approved as part of our authorization process.

SA-04: ACQUISITION PROCESS

Number
SA-04

Family
System and Services Acquisition

Name
ACQUISITION PROCESS

Baseline
Low; Moderate; High

Description
The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

a. Security functional requirements;
b. Security strength requirements;
c. Security assurance requirements;
d. Security-related documentation requirements;
e. Requirements for protecting security-related documentation;
f. Description of the information system development environment and environment in which the system is intended to operate; and
g. Acceptance criteria.

NIST Guidance
Information system components are discrete, identifiable information technology assets (e.g., hardware, software, or firmware) that represent the building blocks of an information system. Information system components include commercial information technology products. Security functional requirements include security capabilities, security functions, and security mechanisms. Security strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass. Security assurance requirements include: (i) development processes, procedures, practices, and methodologies; and (ii) evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required security strength has been achieved. Security documentation requirements address all phases of the system development life cycle.

Security functionality, assurance, and documentation requirements are expressed in terms of security controls and control enhancements that have been selected through the tailoring process. The security control tailoring process includes, for example, the specification of parameter values through the use of assignment and selection statements and the specification of platform dependencies and implementation information. Security documentation provides user and administrator guidance regarding the implementation and operation of security controls. The level of detail required in security documentation is based on the security category or classification level of the information system and the degree to which organizations depend on the stated security capability, functions, or mechanisms to meet overall risk response expectations (as defined in the organizational risk management strategy). Security requirements can also include organizationally mandated configuration settings specifying allowed functions, ports, protocols, and services. Acceptance criteria for information systems, information system components, and information system services are defined in the same manner as such criteria for any organizational acquisition or procurement. The Federal Acquisition Regulation (FAR) Section 7.103 contains information security requirements from FISMA.

Related controls: CM-6, PL-2, PS-7, SA-3, SA-5, SA-8, SA-11, SA-12.

References: HSPD-12; ISO/IEC 15408; FIPS Publications 140-2, 201; NIST Special Publications 800-23, 800-35, 800-36, 800-37, 800-64, 800-70, 800-137; Federal Acquisition Regulation; Web: www.niap-ccevs.org, fips201ep.cio.gov, www.acquisition.gov/far.

DHSS Guidance

This control is implemented at the organizational level by the Department Security Office.

Check with your Department Security Office to make sure they are doing this and have created an organizational authorization package that you can inherit this control from. If not, remind them that security is a team effort, and that a little work on their part can save a lot of work for everyone else.

System X inherits this control from the DHSS Organization authorization package.

SA-09: EXTERNAL INFORMATION SYSTEM SERVICES

Number
SA-09

Family
System and Services Acquisition

Name
EXTERNAL INFORMATION SYSTEM SERVICES

Baseline
Low; Moderate; High

Description
The organization:

a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
c. Employs defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.

NIST Guidance
External information system services are services that are implemented outside of the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems. FISMA and OMB policy require that organizations using external service providers that are processing, storing, or transmitting federal information or operating information systems on behalf of the federal government ensure that such providers meet the same security requirements that federal agencies are required to meet. Organizations establish relationships with external service providers in a variety of ways including, for example, through joint ventures, business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges. The responsibility for managing risks from the use of external information system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Organizations document the basis for trust relationships so the relationships can be monitored over time. External information system services documentation includes government, service providers, end user security roles and responsibilities, and service-

level agreements. Service-level agreements define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance.

Related controls: CA-3, IR-7, PS-7.

References: NIST Special Publication 800-35.

DHSS Guidance

SC-08: TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Number
SC-08

Family
System and Communications Protection

Name
TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Baseline
Moderate; High

Description
The information system protects the confidentiality and integrity of transmitted information.

NIST Guidance
This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing physical distribution systems) or by logical means (e.g., employing encryption techniques). Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk.

Related controls: AC-17, PE-4.

References: FIPS Publications 140-2, 197; NIST Special Publications 800-52, 800-77, 800-81, 800-113; CNSS Policy 15; NSTISSI No. 7003.

DHSS Guidance

SC-12: CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Number
SC-12

Family
System and Communications Protection

Name
CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Baseline
Low; Moderate; High

Description
The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with requirements defined by Department Chief Security Officer for key generation, distribution, storage, access, and destruction.

NIST Guidance
Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational information systems and certificates related to the internal operations of systems.

Related controls: SC-13, SC-17.

References: NIST Special Publications 800-56, 800-57.

DHSS Guidance
This control talks about the certificates and keys that are used to verify the identity of information systems and encrypt data in transit (and sometimes at rest). You'll need to rely on the expertise of IT personnel to help you figure out if this is being done. If your application is hosted at DHSS, then it should already be set up with certificates and keys that are managed by IT Network Services in a manner that satisfies the requirements of this control.

If your application is hosted by DHSS, you shouldn't need to fill out the implementation section of this control. The control can be inherited from Network Services. Otherwise, if your application is hosted externally, check

with the hosting service to ensure that the requirements of this control are being met and provide supporting documentation.

System X is hosted for us by ACME Industries. This control is met as part of their FedRAMP Moderate certification (attached).

SI-01: SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Number
SI-01

Family
System and Information Integrity

Name
SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Baseline
Low; Moderate; High

Description
The organization:

a. Develops, documents, and disseminates to applicable personnel:
   1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and
b. Reviews and updates the current:
   1. System and information integrity policy within every three hundred sixty-five (365) days; and
   2. System and information integrity procedures within every three hundred sixty-five (365) days.

NIST Guidance
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SI family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

Related control: PM-9.

References: NIST Special Publications 800-12, 800-100.

DHSS Guidance

SI-03: MALICIOUS CODE PROTECTION

Number
SI-03

Family
System and Information Integrity

Name
MALICIOUS CODE PROTECTION

Baseline
Low; Moderate; High

Description
The organization:

a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
c. Configures malicious code protection mechanisms to:
    1. Perform periodic scans of the information system every twenty-four (24) hours and real-time scans of files from external sources at endpoint and/or network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; and
    2. Block and quarantine malicious code and send alerts to the administrator and Department Chief Security Officer in response to malicious code detection; and
d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

NIST Guidance
Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in

custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files.

Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7.

References: NIST Special Publication 800-83.

DHSS Guidance

This control tries to cover a lot of ground, and ends up overlapping other controls a bit, but the main component that you absolutely must have is some kind of anti-virus software. This software needs to be installed basically everywhere in the environment where your application is hosted, and also in the environment where you do your work (on your workstation, laptop, etc).

If your application is hosted by DHSS, then you should already be covered. DHSS and the State of Alaska use the McAfee suite of security products to satisfy the requirements of this control. Otherwise you will need to check with the organization that hosts your app to make sure that they have anti-virus and other malicious code protections in place to satisfy this requirement.

System X is hosted for us by ACME Industries. This control is met as part of their FedRAMP Moderate certification (attached).

SI-04: INFORMATION SYSTEM MONITORING

Number
SI-04

Family
System and Information Integrity

Name
INFORMATION SYSTEM MONITORING

Baseline
Low; Moderate; High

Description
The organization:

a. Monitors the information system to detect:
   1. Attacks and indicators of potential attacks in accordance with State of Alaska and department incident handling policy and procedure; and
   2. Unauthorized local, network, and remote connections;
b. Identifies unauthorized use of the information system through defined techniques and methods;
c. Deploys monitoring devices:
   1. Strategically within the information system to collect organization-determined essential information; and
   2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;
d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
g. Provides unauthorized connection information to the Department Chief Security Officer and applicable stakeholders as appropriate.

NIST Guidance
Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Organizations can monitor information systems, for example, by observing audit activities in real time or

by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. Einstein network monitoring devices from the Department of Homeland Security can also be included as monitoring devices. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless.

Related controls: AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7.

References: NIST Special Publications 800-61, 800-83, 800-92, 800-94, 800-137.

DHSS Guidance

Monitoring the application while it runs is extremely important, but also very technical. You'll need to rely on the expertise of IT personnel to determine if this is being done. If your application is hosted by DHSS at our Juneau or Anchorage data centers, then there is a good chance that this has already been set up. If not, it shouldn't take too much effort to get everything set up.

If you application is hosted by DHSS, then it should have our standard monitoring controls in place. Confirm that the application has been configured to send its logs files to department Splunk servers and that traffic is routed through our NetScaler and CheckPoint systems. If hosted externally, confirm with the third party that these monitoring requirements are being met and provide supporting documentation.

Our application is hosted by DHSS and has been configured to send all logs to Splunk. The application sits behind our CheckPoint firewall/Intrusion Prevention Systems and all web traffic is proxied through the NetScaler.

SI-05: SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Number
SI-05

Family
System and Information Integrity

Name
SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Baseline
Low; Moderate; High

Description
The organization:

a. Receives information system security alerts, advisories, and directives from external organizations on an ongoing basis;
b. Generates internal security alerts, advisories, and directives as deemed necessary;
c. Disseminates security alerts, advisories, and directives to: defined personnel; and
d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

NIST Guidance
The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations.

Related control: SI-2.

References: NIST Special Publication 800-40.

DHSS Guidance
This control is implemented at the organizational level by the Department Security Office.

Check with your Department Security Office to make sure they are doing this and have created an organizational authorization package that you can inherit this control from. If not, remind them that security is a team effort, and that a little work on their part can save a lot of work for everyone else.

System X inherits this control from the DHSS Organization authorization package.

SI-07: SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

Number
SI-07

Family
System and Information Integrity

Name
SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

Baseline
Moderate; High

Description
The organization employs integrity verification tools to detect unauthorized changes to information systems.

NIST Guidance
Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications.

Related controls: SA-12, SC-8, SC-13, SI-3.

References: NIST Special Publications 800-147, 800-155.

DHSS Guidance
It's very important to make sure that that nobody tampers with the servers that run your application. To safeguard against this risk, organizations can use various tools that work in a similar way to burglar alarms: they monitor the servers and send out alerts if there are any unexpected changes.

Check with those who host your information system to make sure that this is being done and provide a summary of how this requirement is being met.

Example: System X is hosted for us by ACME Industries. They use SolarWinds and Tripwire products to monitor and verify the integrity of software, firmware, and data in their environment. Attached is an email from their engineer describing how they are using these products and what they accomplish.

SI-08: SPAM PROTECTION

Number
SI-08

Family
System and Information Integrity

Name
SPAM PROTECTION

Baseline
Moderate; High

Description
The organization:

a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and
b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

NIST Guidance
Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers. Spam can be transported by different means including, for example, electronic mail, electronic mail attachments, and web accesses. Spam protection mechanisms include, for example, signature definitions.

Related controls: AT-2, AT-3, SC-5, SC-7, SI-3.

References: NIST Special Publication 800-45.

DHSS Guidance
These days, SPAM is one of our biggest security risks. Most State of Alaska email is currently being handled through the ETS Enterprise Exchange email system which has been set up with various SPAM protection mechanisms fulfilling the requirements of this control.

If ETS Enterprise Exchange is the only email system used by the application, then this control should be inherited from an organizational authorization package that includes that email system. Alternately, if there is no email involved with this application, just mark this control as Not Applicable. Otherwise, if your application uses a non-standard mail service, talk to the Security Office about how they would like the information entered into Archer.

System X inherits this control from the ETS Enterprise Exchange authorization package.

SI-10: INFORMATION INPUT VALIDATION

Number
SI-10

Family
System and Information Integrity

Name
INFORMATION INPUT VALIDATION

Baseline
Moderate; High

Description
The information system checks the validity of defined information inputs.

NIST Guidance
Checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. Software applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the tainted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.

References: None.

DHSS Guidance

Appendix A – Acronyms and Abbreviations

Acronym	Term
AC	Access Control
ACA	Patient Protection and Affordable Care Act of 2010
AD	Microsoft Active Directory
ADFS	Active Directory Federation Services
AES	Advanced Encryption Standard
APIPA	Automatic Private IP Addressing
AT	Awareness and Training
AU	Audit and Accountability
CA	Security Assessment and Authorization
CCB	Change Control Board
CFR	Code of Federal Regulations
CI	Configuration Item
CIO	Chief Information Officer
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CM	Configuration Management
CMS	Centers for Medicare & Medicaid Services
CMRS	Continuous Monitoring and Risk Scoring
CMSR	CMS Minimum Security Requirements

Acronym	Term
LAN	Local area network
MA	Maintenance
MARS	Minimum Security Controls for Exchanges – Exchange Reference Architecture Supplement
MITA	Medicaid Information Technology Architecture
MP	Media Protection
NCP	National Checklist Program
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OS	Operating System
OMB	Office of Management and Budget
PDA	Personal digital assistants
PE	Physical and Environmental Protection
PHI	Protected Health Information
PHR	Personal Health Record
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PL	Planning
PM	Information Security Program Plan

Acronym	Term
COOP	Continuity of Operations Plan
CP	Contingency Planning
DES	Data Encryption Standard
DHSS	Department of Health and Social Services
DIFSLA	IRS Publication 3373 Disclosure of Information to Federal, State, and Local Agencies
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DoS	Denial of Service
DPA	Division of Public Assistance
DR	Disaster Recovery
DSO	Department Security Office
EIS-R	Eligibility Information System – Replacement
EPHI	Electronic protected health information
ESI	Electronically Stored Information
FIPS	Federal Information Processing Standards
FTI	Federal Tax Information
GSS	General Support Systems
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH	Health Information Technology for Economic and Clinical Health

Acronym	Term
POA	Plan of Action
POA&M	Plan of Action and Milestones
PS	Personnel Security
PUB	Publication
RA	Risk Assessments
RAC-F	Resource Access Control Facility
ROB	Rules of Behavior
RSS	Registration Support Specialist
SA	System and Services Acquisition
SAR	Safeguard Activity Report
SAM	Security Access Manager
SC	System and Communications Protection
SDLC	Software Development Lifecycle
SFTP	Secure File Transfer Protocol
SI	System and Information Integrity
SOA	State Of Alaska
SSA	Social Security Administration
SSL	Secure Sockets Layer
SSN	Social Security Number
SSO	State Security Office

Acronym	Term
HTTPS	Hypertext Transfer Protocol Secure
IA	Identification and Authentication
ID	Identifier
IDS	Intrusion detection system
INR	Incident Response Report
IP	Internet Protocol
IPSec	Internet Protocol Security
IR	Incident Response
IRS	Internal Revenue Service
IRT	Incident Response Team
IS	Information Security
ISO	International Organization for Standardization
IT	Information Technology

Acronym	Term
SSP	System Security Plan
TLS	Transport Layer Security
URL	Uniform Resource Locator
USGCB	U.S. Government Configuration Baselines
VLAN	Virtual Local Area Network
VM	Vulnerability Management
VPN	Virtual Private Network
WAN	Wide Area Network
WAP	Wireless Access Points
WP	Worker Portal